Asymptotic behavior of an affine random recursion in $\mathbf{Z}_p^k$ defined by a matrix with an eigenvalue of length 1

Claudio Asci

Dipartimento di Matematica e Informatica

Università degli Studi di Trieste

Abstract

In this paper we study the rate of convergence of the Markov chain $\mathbf{X}_{n+1} = A\mathbf{X}_n + \mathbf{B}_n \pmod{p}$, where A is an integer matrix with nonzero eigenvalues, and $\{\mathbf{B}_n\}_n$ is a sequence of independent and identically distributed integer vectors, with support not parallel to a proper subspace of $\mathbf{Q}^k$ invariant under A. If A has an eigenvalue of length 1, then $n = O\left(p^2\right)$ steps are necessary and sufficient to have $\mathbf{X}_n$ sampling from a nearly uniform distribution. In general, if no assumptions on the eigenvalues of A are done, then $O\left(p^2\right)$ steps are sufficient.

Running head. Affine random recursions in $\mathbf{Z}_p^k$.[1]

[1]**MSC 2000 subject classifications.** Primary 60B15; secondary 60J10.

Key words and phrases. Finite state Markov chains; Fourier transform; generating random vectors; rate of convergence.

1 Introduction

In this paper, we study the Markov chain on $\mathbf{Z}^k$ defined by the affine recursion

$$\mathbf{X}_{n+1} = A\mathbf{X}_n + \mathbf{B}_n \pmod p, \tag{1}$$

where $\mathbf{X}_0 = \mathbf{x}_0 \in \mathbf{Z}^k$, $A \in GL_k(\mathbf{Q}) \cap M_k(\mathbf{Z})$, p is an integer, and $\{\mathbf{B}_n\}_n$ is a sequence of independent and identically distributed integer vectors.

Several results on this recursion have been obtained in the mathematical literature. In particular, if $k = 1$ and $\mathbf{B}_n$ is a fixed integer b, for particular values of p (for example, $p = 2^{31} - 1$ or $p = 2^{32}$), the sequence (1) is used to produce pseudorandom numbers on computers. These matters can be found in the book [10].

In [1], [4], and [8], the term b is a random variable B_n chosen with the same probability at each step, and so the authors study the following Markov chain:

$$X_{n+1} = aX_n + B_n \pmod p,$$

where $a \in \mathbf{N}^*$. The aim of these studies is to produce uniformly distributed random numbers on the set $\{0, 1, ..., p-1\}$. In [4], it is shown that, for $a = 2$, $n = O(\ln p \ \ln\ln p)$ steps are sufficient to sample X_n from a distribution almost uniform. Moreover, if $a = 1$, then $n = O\left(p^2\right)$ steps are necessary and sufficient. In [7], also the integer a is a random variable A_n, but the same estimate $n = O(\ln p \ \ln\ln p)$ for the number of steps sufficient is found.

In [2] and in [9], the extension of the previous results to the higher-dimensional case is done, but the recursion (1) is studied only in some particular cases on the distribution of $\mathbf{B}_n$ and on the eigenvalues of A. In the paper [3], the conditions on $\mathbf{B}_n$ are the most general ($\|\mathbf{B}_n\|_\infty \in L^2$ and the support of the distribution of $\mathbf{B}_n$ cannot be parallel to any proper subspace of $\mathbf{Q}^k$ invariant under A). The results of the paper depend on the size of the complex eigenvalues of A. If $|\lambda_i| \neq 1$ for all eigenvalues λ_i, then $n = O\left((\ln p)^2\right)$ steps are sufficient and $n = O(\ln p)$ steps are necessary to reach the uniform distribution. Conversely, if A has an eigenvalue of length 1, only some particular results are obtained.

In this paper, we improve and complete the study begun in [2] and [3] and we provide some results that agree with the one-dimensional case studied in [4]. In general, we prove that, without any assumptions on the eigenvalues of A, $n = O(p^2)$ steps are sufficient to achieve randomness (Theorem 3.1). This theorem generalizes Theorems 4.1 in [2] and 3.9 in [3]. In particular, if A has an eigenvalue of length 1, then $O\left(p^2\right)$ steps are also necessary (Theorem 3.3). This theorem generalizes Theorem 3.11 in [3].

In Sect. 2, we provide some preliminary results and we recall shortly the theory of the random walks on groups. In Sect. 3, we expose the main results of our work, and in Sect. 4 we introduce some problems for further study.

2 Preliminary results

The aim of this paper is to prove that, with some conditions on p and on $\mathbf{B}_n$, the distribution of the Markov chain $\{\mathbf{X}_n\}$ tends to the uniform distribution on $\mathbf{Z}_p^k$, as $n \to +\infty$, where $\{\mathbf{X}_n\}$ is defined by (1), and so it can be supposed on $\mathbf{Z}_p^k$. Moreover, we wish to estimate the rate of convergence of the process.

Set $P_n(\mathbf{x}) = P(\mathbf{X}_n = \mathbf{x})$, $\forall\ \mathbf{x} \in \mathbf{Z}_p^k$, and $\mu(\mathbf{x}) = P(\mathbf{B}_n = \mathbf{x})$, $\forall\ \mathbf{x} \in \mathbf{Z}^k$, $\forall\ n \in \mathbf{N}$; moreover, denote by U the uniform distribution on $\mathbf{Z}_p^k$. Define:

$$V = \{\mathbf{x} \in \mathbf{Z}^k : \mathbf{x} = \mathbf{h} - \mathbf{k}, \quad \text{where } \mathbf{h}, \mathbf{k} \in \text{supp } \mu\}.$$

Denote by d, where $d \leq k$, the degree of the minimum polynomial of A. By definition we have:

$$\prod_{i=1}^{d}(A - \lambda_i I) = \prod_{i=1}^{d}({}^tA - \lambda_i I) = 0 \in M_k(\mathbf{Z}), \quad \lambda_i \in \{\lambda_1, ..., \lambda_d\},\ \forall\ i = d+1, ..., k,$$

where $\lambda_1, ..., \lambda_d, ..., \lambda_k$ are the eigenvalues of A. Finally, set:

$$V^{d-1} = \{A^m \mathbf{x} : \mathbf{x} \in V\ , m = 0, 1, ..., d-1\}.$$

We use the Fourier analysis (see for example [5], [6], [11], and [12]). Define the variation distance between P_n and U in the following way:

$$\|P_n - U\| = \frac{1}{2} \sum_{\alpha \in \mathbf{Z}_p^k} |P_n(\alpha) - U(\alpha)|.$$

It is possible to prove that

$$\|P_n - U\| = \frac{1}{2} \sup_{f \in F} |E_{P_n}(f) - E_U(f)| = \max_{A \subset \mathbf{Z}_p^k} |P_n(A) - U(A)|, \tag{2}$$

where $F \equiv \{f : \mathbf{Z}_p^k \longrightarrow \mathbf{C} : \|f\| \leq 1\}$.

Henceforth, our purpose will be to find an upper bound and a lower bound for $\|P_n - U\|$ in terms of n and p. Observe that we can suppose $\mathbf{X}_0 = \mathbf{0}$; in fact, if we denote by $\{\mathbf{Y}_n\}_n$ the sequence defined by (1) and the condition $\mathbf{X}_0 = \mathbf{0}$, we have $\mathbf{X}_n = \varphi_n(\mathbf{Y}_n)$, where the one to one function $\varphi_n : \mathbf{Z}_p^k \longrightarrow \mathbf{Z}_p^k$ is defined by $\varphi_n(\mathbf{x}) = A^n\mathbf{x}_0 + \mathbf{x}$. Moreover:

$$\|P_n - U\| = \|(P_n \circ \varphi_n) - U\|.$$

Let E be a countable group of $\mathbf{R}^k$ and let $f : \mathbf{E} \longrightarrow \mathbf{C}$; define the generalized Fourier transform $\widehat{f} : \mathbf{C}^k \longrightarrow C$ by:

$$\widehat{f}(\alpha) = \sum_{\mathbf{h} \in E} \exp\left(\frac{2\pi i}{p}\langle \mathbf{h}, \mathrm{Re}(\alpha)\rangle\right) f(\mathbf{h}),$$

where $\mathrm{Re}(\alpha)$ is the vector whose components are the real parts of the components of α. Henceforth, we consider only $E = \mathbf{Z}^k$ or $E = \mathbf{Z}_p^k$.

The following lemma is proved in [2] (Lemma 2.5), and also in [5], in a more general case.

Lemma 2.1 (Upper bound lemma)**.**

$$\|P_n - U\|^2 \leq \frac{1}{4} \sum_{\alpha \in \mathbf{Z}_p^k - \{\mathbf{0}\}} |\widehat{P}_n(\alpha)|^2. \tag{3}$$

Lemma 2.2. Suppose that $M \in GL_k(\mathbf{Q}) \cap M_k(\mathbf{Z})$ and $\gcd(\det(M), p) = 1$; then, $M \in GL_k(\mathbf{Z}_p)$.

Proof. By assumption, there exist $k_1, k_2 \in \mathbf{Z}$ such that

$$k_1 \det(M) + k_2 p = 1,$$

from which $k_1 \det(M) = 1 \pmod{p}$. Moreover:

$$M^{-1} = \frac{1}{\det(M)} N,$$

where $N \in M_k(\mathbf{Z})$, and so $M \in GL_k(\mathbf{Z}_p)$. $\square$

The following two results follow from Lemma 2.2 and their proofs are similar to those of Lemmas 3.1 and 3.4 in [2]: the only difference is that α ranges in $\mathbf{C}^k$ instead of $\mathbf{Z}_p^k$.

Lemma 2.3. Suppose that $\gcd(\det(A), p) = 1$, $\mathbf{X}_0 = \mathbf{0}$, $\alpha \in \mathbf{C}^k$. Then:

1)
$$\widehat{P}_n(\alpha) = \prod_{j=0}^{n-1} \widehat{\mu}\left({}^t A^j \alpha\right).$$

2)
$$|\widehat{P}_n(\alpha)|^2 = \prod_{j=0}^{n-1} \left(\sum_{\mathbf{h},\mathbf{i} \in \mathbf{Z}^k} \mu(\mathbf{h})\mu(\mathbf{i}) \cos\left(\frac{2\pi}{p} \left\langle \mathbf{h} - \mathbf{i}, {}^t A^j \operatorname{Re}(\alpha) \right\rangle \right) \right)$$
$$\leq \prod_{j=0}^{n-1} \left(1 - 2\mu(\mathbf{u})\,\mu(\mathbf{v}) + 2\mu(\mathbf{u})\,\mu(\mathbf{v}) \cos\left(\frac{2\pi}{p} \left\langle \mathbf{u} - \mathbf{v}, {}^t A^j \alpha \right\rangle \right) \right),$$

$\forall\, \mathbf{u}, \mathbf{v} \in \operatorname{supp} \mu$.

Lemma 2.4. Suppose that the support of μ is not parallel to a proper subspace of $\mathbf{Q}^k$ invariant under A. Then, there exists a basis $\{\mathbf{y}_1, ..., \mathbf{y}_k\} \subset V^{d-1}$ of $\mathbf{Q}^k$. Furthermore, for all $p \in \mathbf{N}$ such that $\gcd(\det(\mathbf{y}_1 ... \mathbf{y}_k), p) = 1$ and for all $\alpha \in \mathbf{C}^k - (p\mathbf{Z})^k$, there exists $i \in \{1, ..., k\}$ such that $\langle \mathbf{y}_i, \alpha \rangle \neq 0 \pmod{p}$. In particular, if the support of μ is not parallel to a proper subspace of $\mathbf{Q}^k$, we have $\mathbf{y}_1, ..., \mathbf{y}_k \in V$, $\langle \mathbf{y}_i, \alpha \rangle \neq 0 \pmod{p}$, for some $i \in \{1, ..., k\}$.

Henceforth, we denote by B the matrix $(\mathbf{y}_1 ... \mathbf{y}_k)$, where the vectors $\mathbf{y}_1, ..., \mathbf{y}_k$ are defined by Lemma 2.4.

Lemma 2.5. Let $\alpha \in \mathbf{C}^k$. Then:

$$\|P_n - U\| \geq \frac{1}{2} \left| \widehat{P}_n(\alpha) - \widehat{U}(\alpha) \right|.$$

In particular, if $\alpha \in \mathbf{Z}^k - (p\mathbf{Z})^k$, then:

$$\|P_n - U\| \geq \frac{1}{2} \left| \widehat{P}_n(\alpha) \right|.$$

Proof. From (2), we have:

$$\|P_n - U\| = \frac{1}{2} \sup_{\|f\| \leq 1} |E_{P_n}(f) - E_U(f)|.$$

For all $\alpha \in \mathbf{C}^k$, define the following function $f : \mathbf{Z}_p^k \longrightarrow \mathbf{C}$:

$$f(\mathbf{x}) = \exp\left(\frac{2\pi i}{p} \langle \mathbf{x}, \operatorname{Re}(\alpha) \rangle \right).$$

Since $\|f\| = 1$, we obtain:

$$\begin{aligned}
\|P_n - U\| &\geq \frac{1}{2}|E_{P_n}(f) - E_U(f)| \\
&= \frac{1}{2}\left|\sum_{\mathbf{x}\in\mathbf{Z}_p^k} P_n(\mathbf{x})\exp\left(\frac{2\pi i}{p}\langle \mathbf{x}, \mathrm{Re}(\alpha)\rangle\right) - \frac{1}{p^k}\sum_{\mathbf{x}\in\mathbf{Z}_p^k}\exp\left(\frac{2\pi i}{p}\langle \mathbf{x}, \mathrm{Re}(\alpha)\rangle\right)\right| \\
&= \frac{1}{2}\left|\widehat{P}_n(\alpha) - \widehat{U}(\alpha)\right|.
\end{aligned}$$

In particular, if $\alpha \in \mathbf{Z}^k - (p\mathbf{Z})^k$, there exists $j_0 \in \{1, ..., k\}$ such that $\alpha_{j_0} \in \mathbf{Z} - p\mathbf{Z}$; then:

$$\begin{aligned}
\widehat{U}(\alpha) &= \frac{1}{p^k}\prod_{j=1}^{k}\left(\sum_{x_j\in\mathbf{Z}_p}\exp\left(\frac{2\pi i}{p}x_j\alpha_j\right)\right) \\
&= \frac{1}{p^k}\prod_{j\in\{1,...,k\}-j_0}\left(\sum_{x_j\in\mathbf{Z}_p}\exp\left(\frac{2\pi i}{p}x_j\alpha_j\right)\right)\sum_{x_{j_0}\in\mathbf{Z}_p}\exp\left(\frac{2\pi i}{p}x_{j_0}\alpha_{j_0}\right).
\end{aligned}$$

Moreover:

$$\sum_{x_{j_0}\in\mathbf{Z}_p}\exp\left(\frac{2\pi i}{p}x_{j_0}\alpha_{j_0}\right) = \frac{1 - \left(\exp\left(\frac{2\pi i}{p}\alpha_{j_0}\right)\right)^p}{1 - \exp\left(\frac{2\pi i}{p}\alpha_{j_0}\right)} = 0$$

$$\Rightarrow \widehat{U}(\alpha) = 0,$$

from which

$$\|P_n - U\| \geq \frac{1}{2}\left|\widehat{P}_n(\alpha)\right|. \ \square$$

3 Main results

Theorem 3.1. Assume that A has eigenvalues $\lambda_1, ..., \lambda_k \in \mathbf{C}^*$, and assume that the support of μ is not parallel to a proper subspace of $\mathbf{Q}^k$ invariant under A. Then, there exist $\alpha, c \in \mathbf{R}^+$ and $N \in \mathbf{N}$ such that, for all $p \in \mathbf{N}$ such that $p > N$, $\gcd(\det(A), p) = \gcd(\det(B), p) = 1$, and for all $n \geq cp^2$, we have:

$$\|P_n - U\| \leq 2^{k-1}\exp\left(-\frac{\alpha(n-k+1)}{p^2}\right).$$

Proof. For all $s \in \mathbf{N}$, from Lemma 2.3, we have:

$$\sum_{\alpha \in \mathbf{Z}_p^k - \{\mathbf{0}\}} |\widehat{P}_n(\alpha)|^2 \leq \sum_{\alpha \in \mathbf{Z}_p^k - \{\mathbf{0}\}} \prod_{j=0}^{n-s-1} f_s(\alpha, j), \tag{4}$$

where $f_s(\alpha, j) \equiv \left(\sum_{\mathbf{u}, \mathbf{v} \in \mathbf{Z}^k} \mu(\mathbf{u})\mu(\mathbf{v}) \cos\left(\frac{2\pi}{p} \left\langle \mathbf{u} - \mathbf{v}, {}^t A^{j+s} \alpha \right\rangle \right) \right)$.

Observe that, for all $j \in \mathbf{N}$ and for all $\alpha_1, \alpha_2 \in \mathbf{Z}_p^k - \{\mathbf{0}\}$ such that $\alpha_1 \neq \alpha_2$, from Lemma 2.2 we have ${}^t A^j \alpha_1 \neq {}^t A^j \alpha_2 \pmod p$, and so

$$\left\{ {}^t A^j \alpha : \alpha \in \mathbf{Z}_p^k - \{\mathbf{0}\} \right\} = \mathbf{Z}_p^k - \{\mathbf{0}\}.$$

Moreover, use the following result:

Lemma 3.2.

$$\sum_{j=1}^{s} \prod_{i=1}^{r} a_{\pi_i(j)} \leq \sum_{j=1}^{s} a_j^r,$$

where, for all $i = 1, ..., r$ and all $j = 1, ..., s$, π_i is a permutation of $\{1, ..., s\}$ and $a_j \geq 0$.

Then we have:

$$\sum_{\alpha \in \mathbf{Z}_p^k - \{\mathbf{0}\}} \prod_{j=0}^{n-s-1} f_s(\alpha, j) \leq \sum_{\alpha \in \mathbf{Z}_p^k - \{\mathbf{0}\}} f_s(\alpha, 0)^{n-s}. \tag{5}$$

Consider the vectors $\mathbf{y}_1, ..., \mathbf{y}_k$ defined by Lemma 2.4; then, for all $m = 1, ..., k$:

$$\mathbf{y}_m = A^{z_m}(\mathbf{u}_m - \mathbf{v}_m), \quad \text{where } \mathbf{u}_m, \mathbf{v}_m \in \text{supp } \mu, \quad z_m \in \{0, 1, ..., d-1\}.$$

For all $m = 1, ..., k$, set:

$$g(m) = \left(1 - 2\mu(\mathbf{u}_m)\mu(\mathbf{v}_m) + 2\mu(\mathbf{u}_m)\mu(\mathbf{v}_m) \cos\left(\frac{2\pi}{p} \langle \mathbf{y}_m, \alpha \rangle \right) \right)^{n - z_m}.$$

Then:

$$f_{z_m}(\alpha, 0)^{n - z_m} \leq g(m).$$

Let $\overline{m} \in \{1, ..., k\}$ be such that $g(\overline{m}) = \min_{m=1,...,k} g(m)$; by (4) and (5), choosing $s = z_{\overline{m}}$, we have:

$$\sum_{\alpha \in \mathbf{Z}_p^k - \{\mathbf{0}\}} |\widehat{P}_n(\alpha)|^2 \leq \sum_{\alpha \in \mathbf{Z}_p^k - \{\mathbf{0}\}} g(\overline{m}). \tag{6}$$

Moreover, we have the following relation:

$$\mathbf{Z}_p^k - \{\mathbf{0}\} = \bigcup_{\emptyset \neq S \subset \{1,\dots,k\}} Y_S,$$

where, for any $\emptyset \neq S \subset \{1, ..., k\}$:

$$Y_S = \Big\{ \alpha \in \mathbf{Z}_p^k - \{\mathbf{0}\} : \langle \mathbf{y}_m, \alpha \rangle \neq 0 \ (\mathrm{mod}\ p),\ \forall\ m \in S,$$
$$\langle \mathbf{y}_m, \alpha \rangle = 0 \ (\mathrm{mod}\ p),\ \forall\ m \notin S \Big\}.$$

Then, (6) implies:

$$\sum_{\alpha \in \mathbf{Z}_p^k - \{\mathbf{0}\}} |\widehat{P}_n(\alpha)|^2 \leq \sum_{\emptyset \neq S \subset \{1,\dots,k\}} \sum_{Y_S} g(\overline{m})$$

$$\leq \sum_{\emptyset \neq S \subset \{1,\dots,k\}} \sum_{Y_S} \min_{m \in S} \left(1 - 2\mu(\mathbf{u}_m)\mu(\mathbf{v}_m) + 2\mu(\mathbf{u}_m)\mu(\mathbf{v}_m) \cos\left(\frac{2\pi}{p} \langle \mathbf{y}_m, \alpha \rangle \right) \right)^{n - z_m}. \quad (7)$$

If $\emptyset \neq S \subset \{1, ..., k\}$, reorder the set S in the following way:

$$S = \left\{ m_{1,S}, ..., m_{|S|,S} \right\}, \quad \text{where } m_{i,S} < m_{j,S} \Leftrightarrow i < j.$$

Then, for all $h = 1, ..., |S|$:

$$\mathbf{y}_{m_{h,S}} = A^{z_{m_{h,S}}} (\mathbf{u}_{m_{h,S}} - \mathbf{v}_{m_{h,S}}), \quad \text{where } \mathbf{u}_{m_{h,S}}, \mathbf{v}_{m_{h,S}} \in \text{supp}\ \mu, \quad z_{m_{h,S}} \in \{0, 1, ..., d-1\}.$$

Set $\overline{\mathbf{y}}_{h,S} \equiv \mathbf{y}_{m_{h,S}}$, $\overline{\mathbf{u}}_{h,S} \equiv \mathbf{u}_{m_{h,S}}$, $\overline{\mathbf{v}}_{h,S} \equiv \mathbf{v}_{m_{h,S}}$, and $z = \max_{m=1,\dots,k} z_m$. Moreover, set:

$$a_{h,S} = \left\langle \overline{\mathbf{y}}_{h,S}, \alpha \right\rangle.$$

We have:

$$\sum_{Y_S} \min_{m \in S} \left(1 - 2\mu(\mathbf{u}_m)\mu(\mathbf{v}_m) + 2\mu(\mathbf{u}_m)\mu(\mathbf{v}_m) \cos\left(\frac{2\pi}{p} \langle \mathbf{y}_m, \alpha \rangle \right) \right)^{n - z_m}$$

$$\leq \sum_{Y_S} \min_{h=1,\dots,|S|} \left(1 - 2\mu(\overline{\mathbf{u}}_{h,S})\mu(\overline{\mathbf{v}}_{h,S}) + 2\mu(\overline{\mathbf{u}}_{h,S})\mu(\overline{\mathbf{v}}_{h,S}) \cos\left(\frac{2\pi}{p} a_{h,S} \right) \right)^{n-z}$$

$$\leq \sum_{\substack{a_{h,S} \in \mathbf{Z}_p - \{0\}, \\ \forall\ h=1,\dots,|S|}} \prod_{h=1}^{|S|} \left(1 - 2\mu(\overline{\mathbf{u}}_{h,S})\mu(\overline{\mathbf{v}}_{h,S}) + 2\mu(\overline{\mathbf{u}}_{h,S})\mu(\overline{\mathbf{v}}_{h,S}) \cos\left(\frac{2\pi}{p} a_{h,S} \right) \right)^{(n-z)/|S|}$$

$$= \prod_{h=1}^{|S|} \sum_{a_{h,S} \in \mathbf{Z}_p - \{0\}} \left(1 - 2\mu(\overline{\mathbf{u}}_{h,S})\mu(\overline{\mathbf{v}}_{h,S}) + 2\mu(\overline{\mathbf{u}}_{h,S})\mu(\overline{\mathbf{v}}_{h,S}) \cos\left(\frac{2\pi}{p} a_{h,S} \right) \right)^{(n-z)/|S|}. \quad (8)$$

Note that $-1+\cos x \leq -\dfrac{2}{\pi^2}x^2$, for all $x \in [-\pi, \pi]$. Furthermore, if $a_{h,S} \in \mathbf{Z}_p - \{0\}$, we can suppose:

$$a_{h,S} \in \mathbf{Z}^* \cap \left[-\frac{p-1}{2}, \frac{p}{2}\right] \Rightarrow \frac{2\pi}{p} a_{h,S} \in [-\pi, \pi].$$

Then, for all $h = 1, ..., |S|$:

$$\sum_{a_{h,S} \in \mathbf{Z}_p - \{0\}} \left(1 - 2\mu(\overline{\mathbf{u}}_{h,S})\mu(\overline{\mathbf{v}}_{h,S}) + 2\mu(\overline{\mathbf{u}}_{h,S})\mu(\overline{\mathbf{v}}_{h,S}) \cos\left(\frac{2\pi}{p} a_{h,S}\right)\right)^{(n-z)/|S|}$$
$$\leq 2 \sum_{a_{h,S} \in \left(\mathbf{Z} \cap \left[1, \frac{p}{2}\right]\right)} \left(1 - \frac{16}{p^2} \mu(\overline{\mathbf{u}}_{h,S})\mu(\overline{\mathbf{v}}_{h,S}) a_{h,S}^2\right)^{(n-z)/|S|}$$
$$\leq 2 \sum_{a_{h,S} \in \mathbf{N}^*} \exp\left(-\frac{16}{kp^2} \mu(\overline{\mathbf{u}}_{h,S})\mu(\overline{\mathbf{v}}_{h,S})(n-k+1) a_{h,S}^2\right), \tag{9}$$

since $z \leq d-1 \leq k-1$ and $|S| \leq k$.

Let $\overline{\tau} \in (0,1)$ be such that $2\overline{\tau}^3 + \overline{\tau}^2 - 1 = 0$ ($\Leftrightarrow \dfrac{\overline{\tau}^3}{1-\overline{\tau}^2} = \dfrac{1}{2}$), and set:

$$t_{h,S} = \exp\left(-\frac{16}{kp^2} \mu(\overline{\mathbf{u}}_{h,S})\mu(\overline{\mathbf{v}}_{h,S})(n-k+1)\right), \quad \overline{c} = \max_{h,S} \frac{-k \ln \overline{\tau}}{16\mu(\overline{\mathbf{u}}_{h,S})\mu(\overline{\mathbf{v}}_{h,S})}.$$

Let $c > \overline{c}$, $N = \left\lfloor \sqrt{\dfrac{k-1}{c-\overline{c}}} \right\rfloor$, $p > N$, and $n \geq cp^2$; then:

$$n - k + 1 \geq \overline{c}p^2 \Rightarrow t_{h,S} \leq \overline{\tau},$$

from which

$$(9) = 2\left(\sum_{a_{h,S} \in \mathbf{N}^*} t_{h,S}^{a_{h,S}^2}\right) = 2\left(t_{h,S} + \sum_{a_{h,S} \geq 2} t_{h,S}^{a_{h,S}^2}\right) \leq 2\left(t_{h,S} + \sum_{a_{h,S} \geq 2} t_{h,S}^{2a_{h,S}}\right)$$
$$= 2\left(t_{h,S} + \frac{t_{h,S}^4}{1 - t_{h,S}^2}\right) \leq 2t_{h,S}\left(1 + \frac{\overline{\tau}^3}{1-\overline{\tau}^2}\right) = 3t_{h,S}$$

by the definition of $\overline{\tau}$. Then:

$$\sum_{a_{h,S} \in \mathbf{Z}_p - \{0\}} \left(1 - 2\mu(\overline{\mathbf{u}}_{h,S})\mu(\overline{\mathbf{v}}_{h,S}) + 2\mu(\overline{\mathbf{u}}_{h,S})\mu(\overline{\mathbf{v}}_{h,S}) \cos\left(\frac{2\pi}{p} a_{h,S}\right)\right)^{(n-z)/|S|}$$
$$\leq 3\exp\left(-\frac{16}{kp^2} \mu(\overline{\mathbf{u}}_{h,S})\mu(\overline{\mathbf{v}}_{h,S})(n-k+1)\right)$$

$$\Rightarrow \prod_{h=1}^{|S|} \sum_{a_{h,S} \in \mathbf{Z}_p - \{0\}} \left(1 - 2\mu(\overline{\mathbf{u}}_{h,S})\mu(\overline{\mathbf{v}}_{h,S}) + 2\mu(\overline{\mathbf{u}}_{h,S})\mu(\overline{\mathbf{v}}_{h,S}) \cos\left(\frac{2\pi}{p} a_{h,S}\right)\right)^{(n-z)/|S|}$$

$$\leq 3^{|S|} \exp\left(-\frac{2\alpha_S(n-k+1)}{p^2}\right), \quad \text{where } \alpha_S = \frac{8}{k}\sum_{h=1}^{|S|}\mu(\overline{\mathbf{u}}_{h,S})\mu(\overline{\mathbf{v}}_{h,S}).$$

Moreover, from (7) and (8) we have:

$$\sum_{\alpha\in\mathbf{Z}_p^k-\{\mathbf{0}\}} |\widehat{P}_n(\alpha)|^2 \leq \exp\left(-\frac{2\alpha(n-k+1)}{p^2}\right)\sum_{|S|=1}^{k}\begin{pmatrix} k \\ |S| \end{pmatrix} 3^{|S|}$$
$$= \left(4^k-1\right)\exp\left(-\frac{2\alpha(n-k+1)}{p^2}\right),$$

where $\alpha = \min_{\emptyset\neq S\subset\{1,\ldots,k\}} \alpha_S = \frac{8}{k}\min_{h,S}\mu(\overline{\mathbf{u}}_{h,S})\mu(\overline{\mathbf{v}}_{h,S}) = -\frac{\ln\overline{\tau}}{2\overline{c}}$. Then, from (3) we have:

$$\|P_n - U\|^2 \leq \frac{1}{4}\left(4^k-1\right)\exp\left(-\frac{2\alpha(n-k+1)}{p^2}\right)$$
$$\leq 4^{k-1}\exp\left(-\frac{2\alpha(n-k+1)}{p^2}\right),$$

from which

$$\|P_n - U\| \leq 2^{k-1}\exp\left(-\frac{\alpha(n-k+1)}{p^2}\right). \ \square \tag{10}$$

Observe that, for $k=1$, the bound (10) reduces to the following:

$$\|P_n - U\| \leq \exp\left(-\frac{\alpha}{p^2}\right),$$

that agrees with the one-dimensional case studied in [4] (case $a=1$).

The following theorem proves that, if A has an eigenvalue of length 1, then $O\left(p^2\right)$ steps are also needed to reach the uniform distribution.

Theorem 3.3. Suppose that the matrix A has an eigenvalue $\lambda\in\mathbf{C}$ such that $|\lambda|=1$ (hence, so does the matrix ${}^tA$), that the support of μ is not parallel to a proper subspace of $\mathbf{Q}^k$ invariant under A, and that $\|\mathbf{B}_n\|_\infty \in L^2$ for all $n\in\mathbf{N}$. Then, there exist $\gamma, c\in\mathbf{R}^+$ and $N\in\mathbf{N}$ such that, for all $p\in\mathbf{N}$ such that $p>N$, $\gcd(\det(A),p)=1$, and for all $n\leq cp^2$, we have:

$$||P_n - U|| \geq \gamma.$$

Proof. By assumption, there exists $\lambda\in\mathbf{C}$ such that ${}^tA\alpha = \lambda\alpha$, for some $\alpha\in\mathbf{C}^k-\{\mathbf{0}\}$.

Case 1: $\mathrm{Re}(\alpha) \neq \mathbf{0}$. From Lemmas 2.3 and 2.5, we have:

$$\|P_n - U\| \geq \frac{1}{2}\left|\widehat{P}_n(\alpha) - \widehat{U}(\alpha)\right| \geq \frac{1}{2}\left(\left|\widehat{P}_n(\alpha)\right| - \left|\widehat{U}(\alpha)\right|\right)$$

$$= \frac{1}{2}\left[\prod_{j=0}^{n-1}\left(\sum_{\mathbf{h},\mathbf{i}\in\mathbf{Z}^K} \mu(\mathbf{h})\mu(\mathbf{i})\cos\left(\frac{2\pi}{p}\left\langle \mathbf{h}-\mathbf{i}, {}^t A^j \,\mathrm{Re}(\alpha)\right\rangle\right)\right)^{1/2} - \left|\frac{1}{p^k}\sum_{\mathbf{x}\in\mathbf{Z}_p^k}\exp\left(\frac{2\pi i}{p}\langle \mathbf{x}, \mathrm{Re}(\alpha)\rangle\right)\right|\right].$$

Since $\cos x \geq 1 - \frac{x^2}{2}$ for all $x \in \mathbf{R}$, we have:

$$\prod_{j=0}^{n-1}\left(\sum_{\mathbf{h},\mathbf{i}\in\mathbf{Z}^K} \mu(\mathbf{h})\mu(\mathbf{i})\cos\left(\frac{2\pi}{p}\left\langle \mathbf{h}-\mathbf{i}, {}^t A^j \,\mathrm{Re}(\alpha)\right\rangle\right)\right)^{1/2}$$

$$\geq \prod_{j=0}^{n-1}\left(1 - \frac{\rho\left\|{}^t A^j \,\mathrm{Re}(\alpha)\right\|_\infty^2}{p^2}\right)^{1/2}, \tag{11}$$

where $\rho = 2\pi^2 k^2 \sum_{\mathbf{h},\mathbf{i}\in\mathbf{Z}^K} \mu(\mathbf{h})\mu(\mathbf{i})\,\|\mathbf{h}-\mathbf{i}\|_\infty^2 \in \mathbf{R}^+$.

Denote by $\overline{\alpha}$ the vector whose components are the complex conjugated values of the components of α; then:

$$\begin{aligned}
&{}^t A\overline{\alpha} = \overline{{}^t A\alpha} = \overline{\lambda\alpha} = \overline{\lambda}\overline{\alpha} \\
&\quad\Rightarrow {}^t A^j \,\mathrm{Re}(\alpha) = {}^t A^j\,\frac{\alpha+\overline{\alpha}}{2} = \frac{\lambda^j\alpha + \overline{\lambda}^j\overline{\alpha}}{2} \\
&\quad\Rightarrow \left\|{}^t A^j \,\mathrm{Re}(\alpha)\right\|_\infty^2 \leq \frac{\left(\|\alpha\|_\infty + \|\overline{\alpha}\|_\infty\right)^2}{4}.
\end{aligned}$$

Moreover, since $\mathrm{Re}(\alpha) \in \mathbf{R}^k - \{\mathbf{0}\}$, for all $p > \|\mathrm{Re}(\alpha)\|_\infty$ we can suppose that $\mathrm{Re}(\alpha) \in$

$\mathbf{R}^k - (p\mathbf{Z})^k$; then, there exists $j_0 \in \{1,...,k\}$ such that $\alpha_{j_0} \in \mathbf{R} - p\mathbf{Z}$, from which:

$$\left|\frac{1}{p^k}\sum_{\mathbf{x}\in\mathbf{Z}_p^k}\exp\left(\frac{2\pi i}{p}\langle\mathbf{x},\mathrm{Re}(\alpha)\rangle\right)\right| = \left|\frac{1}{p^k}\prod_{j=1}^{k}\left(\sum_{x_j\in\mathbf{Z}_p}\exp\left(\frac{2\pi i}{p}x_j\,\mathrm{Re}(\alpha)_j\right)\right)\right|$$

$$= \left|\frac{1}{p^{k-1}}\prod_{j\in\{1,\dots,k\}-j_0}\left(\sum_{x_j\in\mathbf{Z}_p}\exp\left(\frac{2\pi i}{p}x_j\,\mathrm{Re}(\alpha)_j\right)\right)\right|\left|\frac{1}{p}\sum_{x_{j_0}\in\mathbf{Z}_p}\exp\left(\frac{2\pi i}{p}x_{j_0}\,\mathrm{Re}(\alpha)_{j_0}\right)\right|$$

$$\leq \left|\frac{1}{p}\sum_{x_{j_0}\in\mathbf{Z}_p}\exp\left(\frac{2\pi i}{p}x_{j_0}\,\mathrm{Re}(\alpha)_{j_0}\right)\right| = \frac{\left|1-\left(\exp\left(\frac{2\pi i}{p}\,\mathrm{Re}(\alpha)_{j_0}\right)\right)^p\right|}{p\left|1-\exp\left(\frac{2\pi i}{p}\,\mathrm{Re}(\alpha)_{j_0}\right)\right|}$$

$$\leq \frac{\sqrt{2}}{p\sqrt{1-\cos\left(\frac{2\pi}{p}\,\mathrm{Re}(\alpha)_{j_0}\right)}}.$$

Observe that

$$\lim_{p\to+\infty}\frac{\sqrt{2}}{p\sqrt{1-\cos\left(\frac{2\pi}{p}\,\mathrm{Re}(\alpha)_{j_0}\right)}} = \lim_{p\to+\infty}\frac{2}{p\cdot\frac{2\pi}{p}\,\mathrm{Re}(\alpha)_{j_0}} = \frac{1}{\pi\,\mathrm{Re}(\alpha)_{j_0}}.$$

Then, for sufficiently large p and since α is an eigenvector of ${}^tA$, we can suppose that

$$\left|\frac{1}{p^k}\sum_{\mathbf{x}\in\mathbf{Z}_p^k}\exp\left(\frac{2\pi i}{p}\langle\mathbf{x},\mathrm{Re}(\alpha)\rangle\right)\right| \leq \frac{1}{3\,\mathrm{Re}(\alpha)_{j_0}} < 1,$$

from which

$$\|P_n - U\| \geq \frac{1}{2}\left[\left(1-\frac{\rho\left(\|\alpha\|_\infty+\|\overline{\alpha}\|_\infty\right)^2}{4p^2}\right)^{n/2} - \frac{1}{3\,\mathrm{Re}(\alpha)_{j_0}}\right].$$

Moreover, there exists $d \in \mathbf{R}^+$ such that $1 - x \geq \exp(-2x)$, for all $x \in [0,d]$. For sufficiently large p, we can suppose that $\dfrac{\rho\left(\|\alpha\|_\infty+\|\overline{\alpha}\|_\infty\right)^2}{4p^2} \in [0,d]$; hence:

$$||P_n - U|| \geq \frac{1}{2}\left[\exp\left(-\frac{\rho\left(\|\alpha\|_\infty+\|\overline{\alpha}\|_\infty\right)^2 n}{4p^2}\right) - \frac{1}{3\,\mathrm{Re}(\alpha)_{j_0}}\right].$$

Let $\overline{c} \in \mathbf{R}^+$ be such that

$$\exp\left(-\overline{c}\right) > \frac{1}{3\,\mathrm{Re}(\alpha)_{j_0}}$$

and suppose that $n \leq cp^2$, where $c = \dfrac{4\overline{c}}{\rho\left(\|\alpha\|_\infty+\|\overline{\alpha}\|_\infty\right)^2}$. Then, we have:

$$||P_n - U|| \geq \frac{1}{2}\left(\exp\left(-\overline{c}\right) - \frac{1}{3\,\mathrm{Re}(\alpha)_{j_0}}\right) \equiv \overline{\gamma} \in \mathbf{R}^+.$$

Case 2: $\mathrm{Re}(\alpha) = \mathbf{0}$. In this case, $\mathrm{Im}(\alpha) \in \mathbf{R}^k - \{\mathbf{0}\}$, ${}^tA\,\mathrm{Im}(\alpha) = \lambda\,\mathrm{Im}(\alpha)$, and so $\lambda \in \{-1, 1\}$, which implies $\alpha \in \mathbf{Q}^k - \{\mathbf{0}\}$; then, there exists $\mathbf{x} \in \mathbf{Z}^k - \{\mathbf{0}\}$ such that ${}^tA\mathbf{x} \in \{-\mathbf{x}, \mathbf{x}\}$, and so, for all $j \in \mathbf{N}$, ${}^tA^j\mathbf{x} \in \{-\mathbf{x}, \mathbf{x}\}$. For all $p > \|\mathbf{x}\|_\infty$, we can suppose that $\mathbf{x} \in \mathbf{Z}^k - (p\mathbf{Z})^k$; then, from Lemmas 2.3 and 2.5, we have:

$$\begin{aligned}
\|P_n - U\| &\geq \frac{1}{2}\left|\widehat{P}_n(\mathbf{x})\right| \\
&= \frac{1}{2}\prod_{j=0}^{n-1}\left(\sum_{\mathbf{h},\mathbf{i}\in\mathbf{Z}^k}\mu(\mathbf{h})\mu(\mathbf{i})\cos\left(\frac{2\pi}{p}\left\langle \mathbf{h}-\mathbf{i}, {}^tA^j\mathbf{x}\right\rangle\right)\right)^{1/2} \\
&= \frac{1}{2}\left(\sum_{\mathbf{h},\mathbf{i}\in\mathbf{Z}^k}\mu(\mathbf{h})\mu(\mathbf{i})\cos\left(\frac{2\pi}{p}\langle \mathbf{h}-\mathbf{i}, \mathbf{x}\rangle\right)\right)^{n/2}.
\end{aligned}$$

By proceeding as in the proof of the previous case, we obtain the following formula, analogous to (11):

$$||P_n - U|| \geq \frac{1}{2}\left(1 - \frac{\delta}{p^2}\right)^{n/2},$$

where $\delta = 2\pi^2k^2\,\|\mathbf{x}\|_\infty^2 \sum_{\mathbf{h},\mathbf{i}\in\mathbf{Z}^K}\mu(\mathbf{h})\mu(\mathbf{i})\,\|\mathbf{h}-\mathbf{i}\|_\infty^2 \in \mathbf{R}^+$. Finally, for all p sufficiently large:

$$||P_n - U|| \geq \frac{1}{2}\exp\left(-\frac{\delta n}{p^2}\right).$$

Then, for all $n \leq cp^2$, we have:

$$||P_n - U|| \geq \frac{1}{2}\exp\left(-\delta c\right) \equiv \overline{\overline{\gamma}} \in \mathbf{R}^+.$$

From the cases 1 and 2, we have the statement, with $\gamma = \min\{\overline{\gamma}, \overline{\overline{\gamma}}\}$. $\square$

4 Problems for further study

In this paper, we complete the study of the recursion (1) when the Markov chain $\{\mathbf{X}_n\}$ ranges in $\mathbf{Z}_p^k$, but the study of the analogous recursion in $\mathbf{R}^k$ reduced modulo p, for some real number p, is an open problem. Moreover, the sequence (1) can be generalized and replaced by the following:

$$\mathbf{X}_{n+1} = f(\mathbf{X}_n) + \mathbf{B}_n \pmod p, \tag{12}$$

where $f : \mathbf{R}^k \longrightarrow \mathbf{R}^k$ is a one to one function such that $\|f\|_\infty < +\infty$.

We think that, by using the Fourier transform defined by an integral on $\mathbf{R}^k$ instead of a sum on $\mathbf{Z}^k$ or $\mathbf{Z}_p^k$, it is possible to generalize the lemmas in Sect. 2, and to prove the convergence in law of the Markov chain (12) to the uniform distribution on some subset of $\mathbf{R}^k$ (mod p), the set where the chain ranges. This set can be different from $\mathbf{R}^k$ (mod p), and it can be also countable (for example, in the case where the recursion (12) reduces to (1)), then it is necessary to develop a theory and to establish it. Another problem is to estimate the rate of convergence of the Markov chain: the idea is to use the arguments of functional analysis that generalize the theory of the eigenvalues and the eigenvectors of a matrix.

References

[1] Aldous, D., and Diaconis, P. (1986). Shuffling cards and stopping times. *American Mathematical Monthly* **93**, 333-348.

[2] Asci, C. (2001). Generating uniform random vectors. *J. Theoret. Probab.* **14**(2), 333-356.

[3] Asci, C. (2008). Generating uniform random vectors in $\mathbf{Z}_p^k$: the general case. *J. Theoret. Probab.* (to appear).

[4] Chung, F.R.K., Diaconis, P., and Graham, R.L. (1987). Random walks arising in random number generation. *Ann. Probab.* **15**(3), 1148-1165.

[5] Diaconis, P. (1988). *Group Representations in Probability and Statistics.* Institute of Mathematical Statistics, Hayward, California.

[6] Helleloid, G. (2007). *Automorphism Groups of Finite p-Groups: Structure and Applications.* Ph.D. thesis, Department of Mathematics, Stanford University.

[7] Hildebrand, M. (1993). Random processes of the form $X_{n+1} = a_n X_n + b_n$ (mod p). *Ann. Probab.* **21**(2), 710-720.

[8] Hildebrand, M. (1990). *Rates of Convergence of Some Random Processes on Finite Groups.* Ph.D. thesis, Department of Mathematics, Harvard University.

[9] Hildebrand, M., and McCollum, J. (2008). Generating random vectors in $(\mathbf{Z}/p\mathbf{Z})^d$ via an affine random process. *J. Theoret. Probab.* (to appear).

[10] Knuth, D.E. (1981). *The Art of Computer Programming* **2**, 2nd ed. Addison -Wesley, Reading, Massachusetts.

[11] Rosenthal, J.S. (1995). Convergence rates for Markov chains. *Siam Review* **37**(3), 387-405.

[12] Serre, J.P. (1977). *Linear Representations of Finite Groups.* Springer-Verlag, New York.

Claudio Asci, Dipartimento di Matematica e Informatica, Università degli Studi di Trieste, Via Valerio 12/1, 34127 Trieste, Italy

E-mail: asci@dmi.units.it